The Honorable Tim Murphy

1. In your testimony, you recommend that in order to advance health privacy and public health and safety, redrafting some of the public purpose exceptions to the privacy rule to make them more explicit would make sense. Can you please explain how your recommendation could be implemented?

Several of the Privacy Rule's 12 public purpose exceptions, 45 C.F.R. § 164.512, do not provide adequate detail to apprise covered entities about the permissible uses and disclosures of protected health information (PHI). Perhaps the best example is the provision permitting uses and disclosures of PHI "to avert a serious threat to health or safety," which plays a central role in the disclosure of mental health information. The regulation, 45 C.F.R. § 164.512(j), provides, in pertinent part:

> (j) *Standard: uses and disclosures to avert a serious threat to health or safety.*
> (1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:
> (i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
> (B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat . . .

This section of the Privacy Rule is related to the *Tarasoff* duty to warn imposed on mental health professionals. (*Tarasoff v. Regents of the University of California*, 551 P.2d 334 (Cal. 1976))Yet, there is no single *Tarasoff* duty to warn, but 50 different jurisdiction-specific duties and various provisions contained in professional codes of ethics. According to the National Conference of State Legislatures, 29 states have laws mandating the reporting of serious threats, 16 states have permissive reporting laws, 4 states have no duty to report, and 1 state is listed as “other.” (www.ncsl.org/issues-research/health/mental-health-professionals-duty-to-warn.aspx) Other provisions of state laws vary widely. For example, some states apply different

standards to different professionals (e.g., psychologists, social workers); other states differ on the circumstances when warnings are appropriate or vary in the individuals or entities that must be warned; and some states have immunity provisions if certain statutory requirements are followed. Consequently, the average person reading the applicable Privacy Rule provision would have no idea whether there was a privilege to breach confidentiality and/or a duty to warn without consulting a lawyer with special knowledge of the Privacy Rule and the particular state's privacy and duty-to-warn laws.

Even though it was not intended by either Congress in the HIPAA statute or the Department of Health and Human Services (HHS) in its rulemaking, the Privacy Rule has become the *de facto* legal standard for health privacy throughout the U.S. Accordingly, it is not good enough to have a series of broadly worded, "permissive" public purpose exceptions in the Privacy Rule. It is not good enough to say that disclosures are permitted, "consistent with applicable law and standards of ethical conduct," when these other sources of disclosure obligations are often indecipherable. It is especially not good enough to have a vague and inconsistent legal standard applied to serious threats to public health or safety. A reasonable, uniform, national standard should be adopted and implemented.

From a legal standpoint, achieving a national standard is a complex problem, but not an insoluble one. The Privacy Rule provision on averting a serious risk to health or safety, 45 C.F.R. 164.512(j), combines two related issues. The first issue is raised *explicitly* by this part of the Privacy Rule: When is it permissible under the Privacy Rule for a health care provider to breach confidentiality and disclose PHI to avert a serious threat to health or safety? The second issue is raised *implicitly* by this section of the Privacy Rule: When does a health care provider have an affirmative duty to act to avert a serious threat to health or safety, the so-called "duty to warn"? The Privacy Rule's lack of specificity and its policy of deferring to "applicable law and standards of ethical conduct" serve to conflate the issues of breaching confidentiality and duty to warn; it also mixes federal and state law with professional standards to create an unintelligible morass. Most tragically, because of this confusion some uninformed and risk-averse mental health care providers may be reluctant to invoke their privilege to breach confidentiality and to exercise their duty to warn. Such reticence could result in the failure to prevent a life-threatening situation.

A helpful way of analyzing the problem is to view the two issues (breaching confidentiality and duty to warn) separately -- at least initially. For reasons of federalism, Congress may not want to enact legislation establishing a national standard for the duty to warn because it involves matters traditionally within the purview of the states. Similarly, because the statutory language in HIPAA only grants HHS limited regulatory powers, HHS would be unable to set a national standard for the duty to warn through rulemaking. Nonetheless, it is possible to achieve the goal of national uniformity for both breaching confidentiality and the duty to warn *indirectly* by utilizing existing federal legislation and a two-step process of harmonization.

First, HHS clearly has the statutory authority to establish rules for when it is permissible under the Privacy Rule for a covered entity to breach confidentiality to avert a serious threat to health or safety. Indeed, HHS already has promulgated such a rule, 45 C.F.R. § 164.512(j), but it needs to be amended. After considering the views of all stakeholders, HHS should amend the current regulation and promulgate an explicit and detailed new regulation providing, for example, that when a psychotherapist or other provider of mental health services makes a reasonable determination that a patient or client constitutes a threat to cause death or serious harm to one's self or another, the provider is permitted, under the Privacy Rule, to disclose PHI to law enforcement personnel, any intended victim or victims, or others who are in a position to avert the harm. HHS should delete the reference to "applicable law and standards of ethical conduct" because it is the source of inconsistency and confusion.

Amendment of the HIPAA Privacy Rule should be accompanied by comprehensive guidance and specific examples. HHS also should work with professional associations, state and local governments, nongovernmental organizations, and consumer groups to provide meaningful notice and information about the amended regulation. The new, presumably more understandable and practical regulation would replace the current regulation.

The second step would involve the states. As noted earlier, the amended regulation would not expressly address the issue of when a health care provider has an affirmative duty to warn. At least initially, the duty to warn would remain a matter of state law, especially with regard to tort liability. Nevertheless, after a new Privacy Rule provision is promulgated with widespread input,

it is foreseeable that many states would move to harmonize their laws with a reasonable and uniform federal regulatory standard. State legislative initiatives to coordinate with the federal regulation are likely to receive strong support from mental health professionals, consumer groups, and the public, because having reasonable and uniform federal and state laws is not only easier for all affected individuals to understand, it is likely to prevent serious risks to safety and thereby save lives.

At the same time the Privacy Rule is amended, all other federal laws and regulations dealing with the disclosure of mental health information and the duty to warn should be amended, as needed, to achieve consistency. Of particular importance is the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, and the implementing regulations issued by the Department of Education, 34 C.F.R. Part 99. FERPA applies to most public and private postsecondary institutions and to the health records of students at campus health clinics. The FERPA regulations provide: "An educational agency or institution may disclose personally identifiable information from an education record to appropriate parties, including parents of an eligible student, in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals." This permissive provision is broadly worded and, unlike the analogous HIPAA Privacy Rule provision, does not require a "serious and imminent threat." [The issue of "imminent threat" is further discussed in the answer to Representative Cassidy's question.] The divergence of the standards for disclosure of confidential information under FERPA and HIPAA further underscores the need for harmonization.

As discussed in my testimony on April 26, 2013, individual health as well as public health and safety are advanced by maintaining strong protections for the privacy and confidentiality of mental health information. At the same time, for the small number of individuals with severe mental illness who constitute a serious threat to self or others, it is essential to have legal standards for health information disclosure that are reasonable, uniform, well understood, and consistently followed. Amending and clarifying the Privacy Rule is the first step in harmonizing federal and state disclosure laws. Coordinated federal and state efforts represent the best chance to reduce the risk of tragic violence while preserving the confidentiality upon which timely and effective mental health treatment depends.

The Honorable Bill Cassidy

1. It seems to me that one of the biggest questions in a doctor's mind when dealing with a patient with a serious mental illness is whether a threat is not only serious, but also "imminent." As countless families have told us, their children were seen by mental health professionals but they were released without information to the parent, seemingly because the doctor detected no imminent threat. Language, including regulations issued in regard to the NICS background check system, do not say "serious and imminent" threat, but only "serious threat." Knowing that HIPAA serves only as a floor for privacy laws (added onto by state laws, etc.), do you believe there would be a negative effect of removing the imminent requirement?

The requirement of an imminent threat appears in the HIPAA Privacy Rule, 45 C.F.R. § 164.512(j)(1)(i)(A), which indicates when it is permissible for a covered entity to breach confidentiality and disclose PHI "to avert a serious threat to health or safety." HHS should amend the Privacy Rule to remove "imminent" from the regulation, because imminence is such a high standard that mental health providers might believe that even a deeply troubled and dangerous person did not expressly indicate that he or she was planning to take imminent action to harm themselves or others. Removing the "imminent" threat language in the Privacy Rule, however, would not resolve the underlying problem of inconsistent standards.

Interestingly, the *Tarasoff* decision does *not* use the word "imminent" to describe the type of threat giving rise to a mental health provider's duty to warn, but many state laws enacted after *Tarasoff* use this language. According to the National Conference of State Legislatures, 17 states and the District of Columbia require that, to establish a duty to warn, a threat must be "imminent" or "immediate." The other states either do not limit the duty to warn based on the imminence of the threat or do not recognize any duty to warn.

Professional codes of ethics do not require that a threat be imminent before mental health information should or may be disclosed. The American Medical Association (AMA) Code of Medical Ethics, § 5.05, which applies to all physicians and not merely psychiatrists, provides: "When a patient threatens to inflict serious physical harm to another person or to himself or herself and there is a reasonable probability that the patient may carry out the threat, the physician should take reasonable precautions for the protection of the intended victim, which

may include notification of law enforcement authorities." Thus, according to the AMA, whenever there is a serious threat, a physician should take action. By contrast, the codes of ethics of mental health specialists are less proscriptive and stringent; they address only disclosure of mental health information and they make disclosure permissive. The American Psychological Association's Ethical Principles of Psychologists and Code of Conduct § 4.05(b)(3) provides that disclosure of confidential information is permitted to "protect the client/patient, psychologist, or others from harm." Similarly, the American Psychiatric Association's Principles of Medical Ethics, § 4, pt. 8, provides: "When, in the clinical judgment of the treating psychiatrist, the risk of danger is deemed to be significant, the psychiatrist may reveal confidential information disclosed by the patient."

Amending the Privacy Rule to remove the imminent threat requirement would permit a wider range of disclosures, but it would not establish a duty to warn. It also would create a conflict between the amended Privacy Rule and 17 state laws. This situation further illustrates the importance of developing a uniform, national standard, as described in the answer to Chairman Murphy's question.

The Honorable Bruce Braley

1. What have we learned from experiences as we move forward and try to create a balanced system that is protecting the public and rights of the patients to get the best possible treatment, when obviously we have been failing them? What can we do about that?

Public policy on mental health treatment needs to pursue the following three objectives: (1) provide prompt, high quality, comprehensive, and continuing mental health treatment for all who need it; (2) maintain the confidentiality of mental health information disclosed within treatment, because without confidentiality many individuals needing mental health treatment will be deterred from seeking it; and (3) in the unusual situation where a mental health patient constitutes a serious threat to self or others, the mental health professional should understand it is not only permissible to breach confidentiality, but there is an affirmative duty to warn in accordance with a clearly articulated, well understood, reasonable, uniform, national standard.

The Honorable G.K. Butterfield

1. Can you please describe how the new program of public and health care provider education and outreach suggested by the National Committee on Vital and Health Statistics could improve patient awareness of their rights to privacy?

First, in the interest of full disclosure, I was a member of the National Committee on Vital and Health Statistics (NCVHS) in 2002 when the recommendation for greater education and outreach was first made to the Secretary of HHS. I supported the committee recommendations then, and I believe the recommendations are even more important now.

The HIPAA Privacy Rule has become largely irrelevant for a large percentage of patients. Under the Privacy Rule, patient consent is not required for uses and disclosures of PHI for treatment, payment, or health care operations. Instead, notice is required. Covered entities are required to provide individuals with a Notice of Privacy Practices, 45 C.F.R. § 164.520(a), and health care providers with a direct treatment relationship must make a good faith effort to obtain the individual's acknowledgement of receipt of the notice, 45 C.F.R. § 164.520(c)(2)(ii). In practice, the HIPAA notices are so long and detailed that patients typically do not read them if they are given them; sometimes individuals are asked to sign an acknowledgement that they received the notice when they never were given one, and in other instances they are asked to sign a statement saying they declined the offer of a notice.

The current system of only sometimes providing patients with a Notice of Privacy Practices -- and having patients who receive them rarely read and understand them -- may do more harm than good by making it seem as if the HIPAA Privacy Rule is a meaningless paperwork requirement with little or no value to the individual patient. The typical patient's unenlightening initial encounter with the Privacy Rule could be easily changed by requiring covered entities to provide patients with a one-page, clearly written summary of patient rights under the Privacy Rule, including such items as the right to view their health record, the right to copy their health record at no cost, the right to request restrictions on disclosures of their PHI, the right to opt-out of a hospital's directory, the right to file a complaint with the Office for Civil Rights, etc. Although these rights are now included in the detailed Notice of Privacy Practices, they are largely inaccessible to patients because of all the other provisions in the Notice of Privacy Practices. Patient rights are meaningless if patients do not know of their existence.

The Privacy Rule was not intended to be merely a set of regulations for disclosures of PHI in the payment chain of the health care industry. By default, it has become the nation's only broadly applicable health privacy law, and that means HHS has a significant responsibility to the public. This responsibility includes making a greater commitment to provide high quality public and professional education, such as producing on-line tutorials and training materials for health professionals and consumer-oriented health privacy materials in a variety of media. HHS also should establish a robust research program to assess the strengths, weaknesses, and effects of the Privacy Rule, which can be used to guide further amendments and clarifications. In 2003, the NCVHS recommended that HHS establish a program to conduct ongoing research on the Privacy Rule. (National Committee on Vital and Health Statistics, Letter to Secretary Tommy G. Thompson, June 25, 2003, www.ncvhs.hhs.gov/03062513h) Ten years later, when the nation's health care system is undergoing major changes, it is hard to understand why there has been no systematic effort to study the effects of the health privacy law applicable to the overwhelming majority of health care providers and patients in the nation.